

REMARKS

Claims 34 through 73 are pending in the application with the present amendments, including new claims 67 through 73.

Applicants wish to thank the Examiner for granting the interview that was conducted by telephone on July 24, 2006. During the interview, the undersigned discussed the status of the currently pending claims and the procedure for responding to the Office Action in view of the following.

The originally filed claims 1-33 were cancelled and replaced by claims 34-66 in the Preliminary Amendment filed February 24, 2006. The Office Action considered and rejected the originally filed claims 1-33 and did not consider the claims as amended in the Preliminary Amendment, which was submitted some days prior to the date that the Office Action was mailed. Because the currently pending claims are similar in content to the originally filed claims, applicants have amended the claims and point out the differences herein between the currently pending claims and the cited references.

Claim 1 was rejected under 35 U.S.C. 103(a) as being obvious over U.S. Patent No. 6,880,081 to Itkis ("Itkis"), in view of U.S. Patent No. 6,687,683 to Harada et al. ("Harada"). Claim 34, submitted in the Preliminary Amendment dated February 24, 2006, was submitted as a rewritten version of claim 1. As amended herein, claim 34 is fully distinguished from *Itkis* and *Harada*. A key feature of the information processing device recited in claim 34 is that once a decryption key has been calculated by the information processing device, it is encrypted using a leaf key unique to the information processing device and then stored in at least one of storage included in the information processing device or on a recording medium. An advantage of the information processing device recited in claim 34 is that unless one has access to the particular key unique to

a given information processing device, one will not be able to decrypt the encrypted decryption key that is stored on the information recording medium. Then, if one somehow succeeded in determining the one unique key by piracy or hacking, for example, that would make it possible only to decrypt the encryption key that is used to encrypt information under control of that one information processing device. The information under control of every other information processing device would still be secure.

By contrast, the combined teachings of *Itkis* and *Harada* fail to teach or suggest the invention as recited in claim 1. *Itkis* neither teaches nor suggests a hierarchical network of nodes in which each information processing device holds a leaf key which is unique with respect to a first key held by any other information processing device within the hierarchical network of nodes. Instead, *Itkis* teaches only the use of group keys to encrypt an encryption key K (col. 9, lns. 43-49). Each group key is not unique to an individual information processing device, but rather, belongs to a group of devices. For example, as described in *Itkis*, in a tree network, a plurality of devices are divided into a plurality of groups and each group is understood to have "as members, all of the groups beneath said group 100 in the tree." (col. 9, lns. 12-16). In the system described in *Itkis*, since each group key belongs to a group, if one such group key becomes known through pirating efforts, the security of the information controlled by all of the information processing devices in the group is jeopardized.

Harada neither teaches nor suggests the features which are lacking in *Itkis* with respect to the invention recited in claim 34. *Harada* is cited by the Examiner merely as showing certain hardware features such as a storage for storing an encrypted decryption key.

Other claims including independent claims 48, 57, and 62 contain recitations similar to those of claim 34, and are believed to be fully distinguished from *Itkis* and *Harada* for at least the same reasons as discussed above.

Moreover, independent claims 43, 44, 45, 58, 59, 63, 64, 65 and 66 contain similar recitations and are believed to be fully distinguished from the references cited against the originally pending claims.

Finally, claims 67 through 73 recite additional features of the invention which are neither taught nor suggested by the references cited against the originally pending claims, and are believed to be fully distinguished therefrom.

Support for the present amendments is provided, *inter alia*, at paragraphs [0129] through [0139] of the Specification and FIGS. 12 and 13.

In view of the above, each of the presently pending claims in this application is believed to be in immediate condition for allowance. Accordingly, the Examiner is respectfully requested to withdraw the outstanding rejection of the claims and to pass this application to issue. If, however, for any reason the Examiner does not believe that such action can be taken at this time, it is respectfully requested that he telephone applicants' attorney at (908) 654-5000 in order to overcome any additional objections which he might have.

If there are any additional charges in connection with this requested amendment, the Examiner is authorized to charge Deposit Account No. 12-1095 therefor.

Dated: August 7, 2006

Respectfully submitted,

By 
Daryl K. Neff
Registration No.: 38,253
LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK, LLP
600 South Avenue West
Westfield, New Jersey 07090
(908) 654-5000
Attorney for Applicants

679458_1.DOC